M & R has alleged a civil conspiracy: the parties are the defendants, the purpose is to unfairly compete with M & R, and the approximate date is September 2003. M & R's Amended Complaint, while exceedingly terse, provides Defendants with notice of what they are charged with.

[7] Turning to Defendants' second argument, we note that M & R has named five corporate defendants and three individual defendants. Under Illinois law, a civil conspiracy cannot exist between a principal and his agent, but it can exist among corporations. *Knorr Brake Corp. v. Harbil, Inc.*, 738 F.2d 223, 230 (7th Cir.1984) (relying on *People ex rel. Fahner v. Carriage Way West, Inc.*, 88 Ill.2d 300, 58 Ill.Dec. 754, 430 N.E.2d 1005 (1981)). The presence of five corporate defendants makes dismissal inappropriate. Accordingly, count five properly states a civil conspiracy claim.

CONCLUSION

For the reasons provided above, we deny Defendants' motion to dismiss in its entirety. (R. 16–1.) This case is hereby set for a status hearing on June 15, 2004 at 9:00 a.m. for the explicit purpose of setting a trial date for this lawsuit.

In the Matter of the Search of: 3817 W. WEST END, FIRST FLOOR CHICAGO, ILLINOIS 60621.

No. 04 M 108.

United States District Court,
N.D. Illinois,
Eastern Division.

May 27, 2004.

Background: Following execution of residential search warrant in connection with tax fraud investigation, resulting in seizure of computer and electronic storage media, government sought relief from District Court's previous order that government submit search protocol prior to conducting laboratory examination of seized items' contents.

Holdings: The District Court, Schenkier, United States Magistrate Judge, held that:

(1) search warrant for computers warrants heightened scrutiny for particularity;

(2) government was required to submit search protocol in instant case, given fact that probable cause was lacking as to some seized documents, and other factors; and

(3) magistrate at time of issuance of warrant for seizure and subsequent search of home computer has authority to require submission of search protocol.

Motion denied.

1. Searches and Seizures ⚿124

Search warrant that violates particularity requirement cannot pass constitutional muster even if warrant application contains particularity information. U.S.C.A. Const.Amend. 4.

2. Searches and Seizures ⚿125

Search warrant authorizing search and seizure of computers warrants heightened scrutiny for compliance with Fourth Amendment's particularity requirement; seizure often precedes search due to difficulty of on-site search, likelihood of intermingled documents outside scope of probable cause is high, and nature of computers allows for refinement of searches in order to comply with particularity requirement. U.S.C.A. Const.Amend. 4.

3. Searches and Seizures ⚿124

Showing of probable cause for search warrant, no matter how strong, does not authorize court to dispense with indepen-

dent requirement of particularity. U.S.C.A. Const.Amend. 4.

4. Searches and Seizures ⚿124

Factors in degree of particularity required for search warrant are whether: (1) probable cause exists to seize all items of particular type described in warrant; (2) warrant sets out objective standards by which executing officers can differentiate items subject to seizure from those which are not; and (3) government was able to describe items more particularly in light of information available to it at time warrant was issued. U.S.C.A. Const.Amend. 4.

5. Searches and Seizures ⚿125

After executing residential search warrant in connection with tax fraud investigation, which sought seizure of any computers and electronic storage media found and contemplated post-seizure laboratory search of seized items, government had to submit search protocol detailing how search would be conducted, in order to satisfy Fourth Amendment's particularity requirement; probable cause was lacking as to some seized documents, warrant failed to set forth objective standards for differentiating files subject to seizure from those that were not, and government made no attempt to show that it could not provide search criteria that would satisfy particularity requirement. U.S.C.A. Const. Amend. 4; 26 U.S.C.A. § 7206(2).

6. Searches and Seizures ⚿125

Magistrate at time of issuance of warrant for seizure and subsequent search of home computer has authority to require, as condition for conducting post-seizure search, that government submit search protocol that attempts to insure that search will meet Fourth Amendment's particularity requirement. U.S.C.A. Const. Amend. 4.

MEMORANDUM OPINION AND ORDER

SCHENKIER, United States Magistrate Judge.

On April 30, 2004, the Court issued a warrant that authorized the search of a home and the seizure of any computers that might be found, but that conditioned the search of the computer's contents upon the government providing the Court with a "search protocol" describing (a) the information the government sought to seize from the computer, and (b) the methods the government planned to use to locate that information without generally reviewing information on the computers that was unrelated to the alleged criminal activity. At the government's request, and so as not to jeopardize its ongoing investigation, the Court granted the government's motion to place the application and supporting affidavit under seal. On May 4, 2004, after the warrant had been executed and a computer and computer disks had been seized, the government orally requested that the Court allow the government to commence its search of the computer hard drive and disks without providing a protocol. The Court declined to do so.

Thereafter, on May 17, 2004, the government filed a written motion to reconsider, *ex parte* and under seal. In a meeting with the government on May 19, 2004, the Court orally denied the motion to reconsider, explaining the basis for its decision. The government requested that the Court make its ruling of record, which we do by this written opinion.

I.

We begin by recounting the relevant background events. Late in the afternoon of April 30, 2004, the government applied for the issuance of a search warrant for a residence at 3817 W. West End in Chicago,

Illinois. The affidavit in support of the application set forth information offered by the government to establish probable cause to believe that Jacqueline Williams (also known by other names) was the occupant of that residence, and that she was engaged in acts of federal income tax fraud, in violation of 26 U.S.C. § 7206(2), in connection with her preparation and filing of federal income tax returns for various individuals during 2002 and 2003.

The government sought authority to search for and to seize certain enumerated items that it claimed would show the alleged tax fraud. However, with respect to any computers or related media (generally referred to hereafter collectively as "computers"), the government sought a warrant authorizing it to seize those items before conducting any search of their contents for evidence of tax fraud (*see* Warrant, Attachment B, ¶¶ 5–8). The government explained that accountants and tax preparers who are engaged in tax fraud often use computers to prepare and retain records of fraudulent returns, that there was reason to believe that computers would be found at the 3817 W. West End residence, that the government would encounter significant obstacles in attempting to search the contents of any computers while at the residence, and that a search of the computers would be better conducted in a laboratory setting.

After reviewing the government's submission, the Court concluded that there was probable cause to believe that a search of Ms. Williams's residence at 3817 W. West End would yield evidence of the alleged federal income tax fraud. Accordingly, the Court informed the government that it would issue a warrant authorizing a search of the residence for items enumerated in Attachment B to the warrant, and the seizure of those items.

However, the Court expressed concern over the request as it pertained to any computers the government might find at the residence. The Court was satisfied by the government's explanation of why a search of the contents of any computers while at the residence might not be practicable, and thus authorized the government to seize any computer without an on-site search of its contents. But, the Court explained to the government that a computer found during the search of a home likely would contain a wide variety of documents having nothing to do with the alleged criminal activity intermingled with documents that might fall within the scope of the alleged criminal activity. The affidavit provided no information that would suggest otherwise. Neither the application nor the affidavit set forth the types of documents relating to the alleged criminal activity that the government expected to find on the computers. Nor did the government's submission describe the means by which the government planned to search the computer, to avoid a general rummaging through all information on the computer, much of which would be irrelevant to the alleged criminal activity. To the contrary, the government represented that its search of the computer might involve "*an examin[ation of] all the stored data* to determine which particular files are evidence or instrumentalities of a crime" (Aff. in Support of Warrant Application, ¶ 36(a)) (emphasis added).

The Court told the government that in order to address these concerns, prior to allowing any search of the contents of the computers, the Court would require the government to provide a protocol outlining the methods it would use to ensure that its search was reasonably designed to focus on documents related to the alleged criminal activity. The purpose of this protocol was to provide the Court with assurance that the search of the computer after its seizure would not consist merely of a random or general examination of other documents—which, on a home computer, might

contain sensitive information regarding health or other personal and private matters completely unrelated to the alleged criminal activity.

At that time, the government did not object to the requirement of a protocol, but asked whether the Court would require it to be provided before signing the warrant authorizing a search. In light of concerns expressed by the government that the search be conducted quickly because Ms. Williams might suspect that her activity had attracted the interest of the government, the Court decided to sign the warrant so that the search could proceed forthwith. However, the Court made clear that if any computer was found, no search of its contents could commence before the government provided the required protocol. The Court made clear that the authority to seize the computers, and ultimately to search them, was conditioned on the government providing the required protocol.

The Court signed the search warrant at 5:40 p.m. on April 30. In order to prevent the ongoing investigation from being compromised, the Court granted the government's request that the application and affidavit submitted in support of the warrant be filed under seal. As reflected on the return of the warrant, the search began the next morning, May 1, 2004, at 7:30 a.m. The inventory attached to the return of the warrant shows that the government seized a number of items in connection with the search: including one computer (a Hewlett Packard Pavilion 700 computer) and an unspecified number of computer disks.

On May 4, 2004, the government met with the Court to discuss the warrant. Attending the meeting were an attorney for the government (a different individual than the attorney who presented the warrant application on April 30), two agents, and an individual identified as the government's computer expert. The government attorney informed the Court that the search had been conducted, and that a computer had been seized. At that time, the government attorney argued that the government should be permitted to search the contents of the computer without providing the Court with any search protocol. The Court asked the government's computer expert about possible protocols, in order to determine whether there was some objection based on the view that a protocol was impracticable. While the Court considered it to be the responsibility of the government to offer the protocol it deemed best tailored to the search, the Court raised with the government possible ways of focusing the search of the computers, including: limiting the search to specific time periods; using key word searches; and/or limiting the search to text files and excluding graphics files. There was nothing in the responses by the government representatives that indicated that there was some technical or practical reason that a protocol could not be provided.[1]

1. The Court notes that, in one respect, the response (or non-response) by the government was quite surprising. When the Court raised the possibility of limiting the search to certain time periods, one of the government representatives stated that such a limitation would not be helpful since the file directory only shows when a document was last saved. The Court then asked the government technical expert whether that problem could not be overcome by examining the ''metadata'' in the computer files, which would show not only the date a document was last saved, but also when the document was first created and (often times) the changes in the documents from the original draft to the final revision. *See* MANUAL FOR COMPLEX LITIGATION FOURTH at 78 (Federal Judicial Center 2004); *see also* THE SEDONA PRINCIPLES at 52 (The Sedona Conference 2004) (''Metadata is information about a particular data set which may describe, for example, how, when, and by whom it was received, created, accessed, and/or modified

What emerged clearly during the discussion was the government position that the Court lacked the authority to require a protocol. The government asserted that having found probable cause for a search, the Court's inquiry was at an end. In aid of that argument, the government analogized the search of a computer hard drive to the search of a file cabinet concerning papers: the government urged that just as the Court could not regulate the manner in which a file cabinet was searched, it could not regulate the conduct of the search of the computer files. The Court explained that it found this analogy unpersuasive, and that the Court believed it had the authority to require the search protocol. Accordingly, the Court reaffirmed that the government could not commence a search of the seized computer without first providing a search protocol.

Two weeks later, on May 17, 2004, the government filed a written motion, asking the Court to reconsider its requirement of a protocol. On May 19, 2004, the Court met informally with the government to discuss the motion. The Court explained that it had considered the government's arguments and authorities, but concluded that the Court possessed the power to require a search protocol, and that the power to do so was properly exercised here.

II.

The government's motion raises a serious question, one which we believe to be of first impression in this district: whether, when deciding to issue a warrant that would involve the seizure and subsequent search of a home computer, a magistrate judge has the authority to require the government to set forth a search protocol that attempts to ensure that the search will not exceed constitutional bounds. For the reasons set forth below, we believe that the answer to that question is yes.

A.

A search warrant may issue only "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. The Supreme Court has interpreted this provision to encompass three requirements: (1) that any warrants "must be issued by neutral, disinterested magistrates"; (2) that those seeking a warrant must show probable cause "to believe that 'the evidence sought will aid in a particular apprehension or conviction' for a particular offense"; and (3) that the warrants describe with particularity the " 'things to be seized,' as well as the place to be searched." *Dalia v. United States*, 441 U.S. 238, 255, 99 S.Ct. 1682, 60 L.Ed.2d 177 (1979).

[1] It is frequently said that the purpose of the particularity requirement is "to prevent a general exploratory rummaging in a person's belongings." *United States v. Carey*, 172 F.3d 1268, 1272 (10th Cir. 1999) (citing *Marron v. United States*, 275 U.S. 192, 196, 48 S.Ct. 74, 72 L.Ed. 231 (1927)); *see also United States v. Stefonek*, 179 F.3d 1030, 1033 (7th Cir.1999) ("one of the purposes of the Fourth Amendment was to outlaw general warrants"). But, the particularity requirement serves another important purpose as well: it "assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search,

and how it is formatted. Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept'"). The government technical expert made no response, leaving the Court with the firm impression that he was not familiar with a term that we would expect a computer expert to know.

and the limits of his power to search." *Groh v. Ramirez,* —— U.S. ——, 124 S.Ct. 1284, 1292, 157 L.Ed.2d 1068 (2004) (quoting *United States v. Chadwick,* 433 U.S. 1, 9, 97 S.Ct. 2476, 53 L.Ed.2d 538 (1977)). When the warrant does not describe with particularity the things to be seized, it will not pass constitutional muster even if the application contains that information. *Groh,* —— U.S. at ——, 124 S.Ct. at 1289 ("The fact that the *application* adequately described the 'things to be seized' does not save the *warrant* from its facial invalidity") (emphasis in original); *see also Stefonek,* 179 F.3d at 1033 ("The Fourth Amendment requires that the *warrant* particularly describe the things to be seized, not the papers presented to the judicial officer . . .") (emphasis in original).

[2] The degree of particularity that is required in any given situation may not be determined by resorting to some simple formulaic approach, but instead "varies depending on the circumstances of the case and the types of items involved." *United States v. Spilotro,* 800 F.2d 959, 963 (9th Cir.1986). A number of courts addressing the issue have found that the search and seizure of a computer requires careful scrutiny of the particularity requirement. *See United States v. Carey,* 172 F.3d 1268, 1275 n. 7 (10th Cir.1999) ("the storage capacity of computers requires a special approach" in assessing the particularity requirement); *United States v. Barbuto,* No. 2:00CR197K, 2001 WL 670930, *4 (D.Utah Apr.12, 2001) ("searches on computers are unique because of their abundant storage capacity and the likelihood of discovering 'intermingled documents' . . ."); *United States v. Hunter,* 13 F.Supp.2d 574, 583–84 (D.Vt.1998) ("Computer searches present the same problem as document searches—the intermingling of relevant and irrelevant material—but to a heightened degree," which requires that each computer search be "independently evaluated for lack of particularity"). Likewise, we believe that a request for the search and seizure of computers merits a close look at the particularity requirement for several reasons.

First, it is frequently the case with computers that the normal sequence of "search" and then selective "seizure" is turned on its head. Because of the difficulties of conducting an on-site search of computers, the government frequently seeks (and, as here, obtains), authority to seize computers without any prior review of their contents.

[3] *Second,* that is significant in this case because of the substantial likelihood that the computer contains an "intermingling" of documents evidencing the alleged tax fraud, with documents that the government has no probable cause to seize. While the warrant application here established probable cause to believe that the computer may contain information of tax fraud, it did not contain information indicating that the computer contains nothing but information of tax fraud. The application contains no evidence that Ms. Williams's computer was dedicated solely to the alleged fraudulent activity; or that every return that Ms. Williams prepared was fraudulent; or that she did not use the computer for the full range of legitimate activities for which people typically use home computers.[2]

2. The government's motion emphasizes that the Court orally stated during the May 4, 2004 meeting that there was ''no question'' that the application demonstrated probable cause for the search (Gov't Mot. to Reconsider, at 2). However, a showing of probable cause—no matter how strong—does not authorize a court to dispense with the independent requirement of particularity. *Groh,* —— U.S. at ——, 124 S.Ct. at 1289 (a warrant that met the probable cause requirement nonetheless was ''plainly invalid'' where it failed to satisfy the particularity requirement).

Third, we consider the extraordinary volume of information that may be stored even on a home computer. A megabyte of memory holds the equivalent of 500 typewritten pages of text. MANUAL FOR COMPLEX LITIGATION § 11.446, at 77. Even a modest home computer today frequently has 512 megabytes of memory (if not more), which translates into capacity of 256,000 pages of information. A floppy disk (some number of which were seized here) has a capacity of 1.44 megabytes, which translates into a capacity of 720 pages of plain text. *Id.* The capacity of the computer to store these large quantities of information increases the risk that many of the intermingled documents will have nothing to do with the alleged criminal activity that creates the probable cause for a search and seizure.

Fourth, while computers present the possibility of confronting far greater volumes of documents than are typically presented in a paper document search, computers also present the tools to refine searches in ways that cannot be done with hard copy files. When confronting a file cabinet full of papers, there may be no way to determine what to seize without doing some level of review of everything in the cabinet, as "few people keep documents of their criminal transactions in a folder marked '[crime] records.'" *Hunter*, 13 F.Supp.2d at 582 (quoting *United States v. Riley*, 906 F.2d 841, 845 (2d Cir.1990)). Thus, in that setting, it may be inevitable that innocuous records must be examined to determine whether they fall into the category of those papers covered by the search warrant. *Andresen v. Maryland*, 427 U.S. 463, 482 n. 11, 96 S.Ct. 2737, 49 L.Ed.2d 627 (1976).

By contrast, computer technology affords a variety of methods by which the government may tailor a search to target on the documents which evidence the alleged criminal activity. These methods include limiting the search by date range; doing key word searches; limiting the search to text files or graphics files; and focusing on certain software programs. *See Carey*, 172 F.3d at 1276. Of course, these are not the exclusive means of focusing a computer search, and they are not the means that might be appropriate in every case. But, the existence of these tools demonstrates the ability of the government to be more targeted in its review of computer information than it can be when reviewing hard copy documents in a file cabinet.[3]

B.

[4] We now consider how these considerations relevant to computer searches affect the particularity requirement in this case. In so doing, we use the factors set forth in *Spilotro* in determining the degree of particularity required: "(1) whether probable cause exists to seize all items of a particular type described in the warrant,

3. In its oral presentation on May 4 (but not in its written motion), the government argued that a search protocol was not required by analogizing to the situation of the search of documents in a file cabinet. For the reasons stated above, we are persuaded that the analogy of the file cabinet to the computer is inadequate for purposes of the Fourth Amendment issue presented here, a conclusion that the *Carey* court also reached. *Carey*, 172 F.3d at 1275 ("Relying on analogies to closed containers or file cabinets may lead courts to 'oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage' ") (citations omitted). Moreover, to the extent the government's analogy suggests that protocols are never used with respect to document searches, that suggestion is incorrect. In *Hunter*, the government's application for a search warrant included a protocol for the execution of the warrant that was designed to minimize the "invasion of materials protected by attorney-client privilege"—whether in hard copy form or residing on a computer hard drive. *Hunter*, 13 F.Supp.2d at 578.

. . .; (2) whether the warrant sets out objective standards by which executing officers can differentiate items subject to seizure from those which are not, . . .; and (3) whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant was issued." *Spilotro,* 800 F.2d at 963. We address each of these factors in turn.

[5] *First,* there is probable cause to believe that there are some documents on the computers that constitute evidence of the alleged criminal activity. However, as explained above, those documents likely are intermingled with other, innocent materials in which the government has no interest. Thus, there is not probable cause to believe that everything on the computers is evidence of the alleged criminal activity.

Second, the warrant—as well as the application—fails to set forth "objective standards by which executing officers can differentiate items subject to seizure from those which are not." *Spilotro,* 800 F.2d at 963. The warrant merely describes the computers and related materials to be seized; it does not specify what objective standards the government proposes to use "to specify what types of files were sought in the searching of the two computers so that personal files would not be searched." *Barbuto,* 2001 WL 670930, *5; *see also Carey,* 172 F.3d at 1275 (when confronting a situation of intermingled computer documents, "law enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in the warrant").

Third, we consider whether the government was able to provide a better description of how it seeks to go about searching the computer for information of criminal activity. " '[G]eneric classifications in a warrant are acceptable only when a more precise description is not possible.' " *United States v. Kow,* 58 F.3d 423, 427 (9th Cir.1995). The government has not even attempted to show that it cannot provide search criteria in the context of this warrant.[4]

In addressing searches for hard copy documents and seizures of telephone communications, the Supreme Court has admonished that "responsible officials, *including judicial officers,* must take care to assure that [searches] are conducted in a manner that minimizes unwarranted intrusion upon privacy." *Andresen,* 427 U.S. at 482 n. 11, 96 S.Ct. 2737 (emphasis added). That admonition applies with even more force in the context of computer searches, where the volume of intermingled documents may be substantial and there are tools to focus those searches that are unavailable for searches of hard copy docu-

4. The government makes a general argument that it would be ''impractical'' for the Court to ''inquire as to how the government will conduct a search'' (Gov't Mot. to Reconsider at 3 n. 1). That argument fails to account for the tools that are available to create protocols to tailor computer searches, as other courts have recognized. The government's argument also fails to acknowledge that the Department of Justice has issued a manual stating that it often will be necessary to provide a search protocol in the context of a computer search: ''The affidavit should also explain what techniques the agents expect to use to search the computer for specific files that represent evidence of crime and may be intermingled with entirely innocuous documents.'' SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, United States Department of Justice, Executive Officer for United States Attorneys, Office of Legal Education at 100 (2d ed.2002) (hereinafter ''DOJ MANUAL''). While the statements in the DOJ Manual do not represent the official position of the Department of Justice or other agencies, DOJ MANUAL at x, at a minimum the Manual further undermines the government's generalized assertion of ''impracticality.''

ments. We conclude that, as a practical matter, the government can provide the Court with a protocol that would supply particularity to the search of the computers. And, we conclude that as a matter of constitutional law, the government must do so in order to satisfy the particularity requirement of the Fourth Amendment.

C.

[6] The government's core objection to providing a search protocol is that the Court is powerless to require it. That objection is inconsistent with the foregoing case law, *see, e.g., Carey* and *Barbuto,* as well as with the DOJ Manual, which notes that "[t]he reasons for articulating the search strategy in the affidavit are both practical and legal." DOJ MANUAL, at 101. Indeed, the government's notion that a judge is powerless to regulate the means of executing a search and seizure is belied by the government's own request in this case that the Court approve one particular method of executing the search: that is, to allow the government to seize the computers so that they may be searched off-site. That request, which is consistent with the position set forth in the DOJ Manual, *see* DOJ MANUAL at 100, 103, recognizes that practical considerations are relevant to delineating the means of a search. That is also the teaching of *Spilotro,* which looks to practical considerations in determining the degree of particularity required in a warrant.

We have considered the government's arguments that the Court lacks the authority to require a search protocol to give particularity to the search and seizure of the computers' contents. We find those arguments unpersuasive.

The government cites several "knock and enter" cases to argue that the Court has no authority to inquire in advance into the methods by which a warrant will be executed. *United States v. Banks,* 540 U.S. 31, 124 S.Ct. 521, 157 L.Ed.2d 343 (2003); *United States v. Basham,* 268 F.3d 1199 (10th Cir.2001). We view these cases as recognizing the reality that neither the government nor a judge can know in advance what situation may confront agents who approach a location to execute a search, and that, as a result, no one can say in advance how many knocks must be made on the door or how long a knock must go unanswered before entry. By contrast, when the government wishes to search a computer hard drive in the controlled environment of a laboratory, it is not confronted with a rapidly evolving and sometimes dangerous situation that must be addressed on the spot.

Nor are we persuaded by the government's citation to *Dalia,* 441 U.S. at 257–58, 99 S.Ct. 1682, in which the Supreme Court held that a warrant authorizing the installation of a wire intercept device was not defective because it failed to specify how the device would be installed. Indeed, while that case did not present the question of a judge's authority to specify the method by which government agents would listen in on intercepted calls, the Supreme Court noted with approval that the court issuing the warrant in fact had ordered the government "to take all reasonable precautions 'to minimize the interception of communications not otherwise subject to interception,' and required the officials to make periodic progress reports." *Dalia,* 441 U.S. at 242, 99 S.Ct. 1682.

Finally, the government argues that having found probable cause and allowing the computers to be seized, the Court can do nothing more (Gov't Mot. to Reconsider, at 6, 8). At the threshold, this argument fails to acknowledge what the government elsewhere in its motion acknowledges (*id.* at 2): that the Court issued the warrant conditioned upon the

government providing the protocol before there was a search of any computers. The Court imposed that requirement as a condition of signing the warrant because without a protocol, the warrant lacked particularity that would justify a search of the computers.

Moreover, the government's argument erroneously conflates the probable cause and particularity requirements. As *Groh* recently reaffirmed in finding invalid a warrant that was based on probable cause but lacked particularity, these are independent requirements which must both be met. Here, while there was (and is) probable cause to believe that the computer contains some information that would constitute evidence of criminal activity, the warrant does not indicate what types of such information the government wishes to search for on the computer or how the government seeks to search for it in a way that will, to adapt the language of the *Dalia* court to the computer context, "minimize the [review] of [information] not otherwise subject to [review]." 441 U.S. at 242, 99 S.Ct. 1682. In short, the Court imposed the requirement of a protocol to ensure that there was both probable cause and particularity before the government searched the computers.

D.

The government urges that any questions about the manner in which a search is executed may be addressed by a judge when approving the warrant, but only when a judge later is confronted with a motion to suppress. If adopted, such an approach would unnecessarily run the risk of the unfortunate results reached in *Carey* and *Barbuto,* where evidence seized in a search of a computer was suppressed because of a failure to provide the magistrate judge with search protocols. *Carey,* 172 F.3d at 1275 (in the case of intermingled documents, the magistrate judge should "require officers to specify in a warrant which type of files are sought"); *Barbuto,* 2001 WL 670930, *5 (methods or criteria by which a search of computer files would be conducted "should have been presented to the magistrate before the issuance of the warrants or to support the issuance of a second, more specific warrant once intermingled documents were discovered").

An approach that leads to such results is neither desirable nor legally required. We do not believe that is the approach that the Supreme Court had in mind when it stated that "responsible officials, including judicial officials," must take care to assure that searches are conducted so as to "minimize[ ] unwarranted intrusions upon privacy." *Andresen,* 427 U.S. at 482 n. 11, 96 S.Ct. 2737. The purpose of review of warrant applications by "neutral, disinterested magistrates" is to ensure that the requirements of probable cause and particularity are met. When there are concerns about the particularity of a given search, as is the case here, it is both sensible and constitutionally required to address those concerns at the front end of the process, and to resolve them in a way that avoids the later suppression of evidence.

CONCLUSION

We emphasize that, in requiring a protocol here, the Court does not seek to dictate the specific criteria that the government may employ in order to supply particularity to its search and seizure of contents of the computers. Nor does the Court envision that a set of criteria initially approved will be forever set in stone; we do not foreclose the possibility that those criteria may need to be adjusted in response to what is found once the computer search commences. But, as matters now stand, what the government seeks is a license to roam through everything in the computer without limitation and without standards. Such a request fails to satisfy the particu-

larity requirement of the Fourth Amendment, and the Court therefore will not approve it.

Accordingly, the Court denies the government's motion to reconsider. In light of this ruling, the Court orders that within 21 days the government inform the Court in writing of the following: (a) whether there is good cause that this Opinion, which does not disclose sensitive material from the application, should remain under seal; and (b) whether the government still wishes to search the computer. If so, within that 21 day period the government shall submit for review a proposed protocol for searching the contents of the computer. If the government informs the Court that it no longer wishes to search the computer, then the Court will direct that the computer be returned.

Michael BABEL, Irina Babel, Evelin Babel and Rostislav Babel, Plaintiffs,

v.

U.S. DEPARTMENT OF HOMELAND SECURITY, Secretary Tom Ridge; United States Citizenship and Immigration Services, Donald J. Monica, Interim District Director, and John Ashcroft, United States Attorney General, Defendants.

No. 02 C 4720.

United States District Court,
N.D. Illinois,
Eastern Division.

June 15, 2004.

Background: Aliens filed application for fees and costs pursuant to the Equal Access to Justice Act (EAJA) after they received a final adjudication on their applications for lawful permanent resident status. The District Court, St.

Holdings: Eve, J., held that:

(1) because aliens did not receive a judgment on the merits, a court ordered consent decree, or any other form of judicial sanction, they could not be considered a prevailing party for purposes of EAJA, and

(2) EAJA barred recovery because federal defendants had a substantial justification for the lengthy adjudication of aliens' applications.

Application denied.

1. United States ⚿147(7, 8.1)

A party must meet the following four requirements before the party can recover under Equal Access to Justice Act (EAJA): (1) if the party is an individual, his net worth must not exceed $2,000,000 at the time the civil action is filed; (2) the party "prevailed" in the action; (3) the position of the United States was not substantially justified; and (4) there are no special circumstances that would make an award unjust. 28 U.S.C.A. § 2412.

2. Federal Civil Procedure ⚿2737.1

Standards used in defining the term "prevailing party" are generally applicable to all fee-shifting statutes that authorize an award of fees and costs to a prevailing party.

3. Federal Civil Procedure ⚿2737.1

For purposes of fee-shifting statutes that authorize an award of fees and costs to a prevailing party, a "prevailing party" is generally one who is granted some relief by the court, concerning a significant issue in the litigation, by either a judgment on